

Le principe d'accountability RGPD

Description

L'entrée en vigueur du [Règlement Général sur la Protection des Données \(RGPD\)](#) est venue introduire certains principes dont le respect est primordial pour tout organisme souhaitant être en conformité.

Parmi eux on retrouve le principe d'accountability ou « responsabilité » en français. Il correspond à une obligation de mise en œuvre des procédures et mécanismes internes permettant de démontrer le respect des règles liées à la protection des données.

[Obtenir un devis gratuit RGPD](#)

Qu'est-ce que le principe d'accountability du RGPD ?

Il convient de définir la notion du principe d'accountability, ainsi que **ses objectifs** et **les personnes** concernées par son application.

La définition du principe d'accountability

Le principe d'accountability correspond à l'obligation pour les entreprises de mettre en œuvre les **mécanismes** et **procédures internes** permettant de démontrer le respect des règles relatives à la protection des données.

Cette obligation permet de s'assurer de l'efficacité des **mesures techniques** et **organisationnelles** mises en place par le responsable de traitement. Les mesures d'accountability doivent être révisées et **mises à jour** régulièrement pour garantir un traitement **conforme** des données.

Le principe d'accountability est assorti de **deux autres principes** visant à assurer le respect du RGPD, à savoir :

- Principe de privacy by default : une fois le produit ou service communiqué au public, les standards de protection des données personnelles devront être appliqués par défaut.
- Principe de [privacy by design](#) : l'entreprise doit intégrer la protection des données à caractère personnel dès la conception de projets rattachés au traitement des

données d'une entreprise.

Les objectifs du principe d'accountability

L'objectif principal de la mise en place du principe d'accountability est de prouver que les **mesures adéquates** ont été adoptées par les entreprises et organismes publics pour être en conformité avec le RGPD. Cette preuve peut notamment être apportée par **une documentation**.

Elle permet également **aux instances de contrôle** de chaque pays membres de l'Union européenne de vérifier le respect des règles de sécurité par **les entreprises et organismes publics**. Le but étant de responsabiliser les entreprises et organismes publics à l'échelle européenne afin de protéger au mieux la vie privée des utilisateurs.

Par ailleurs, le principe d'accountability du RGPD, **le responsable de traitement** doit également répondre aux objectifs suivants :

- Effectuer une analyse des risques
- Appliquer les principes de protection des données afin de sécuriser leur traitement
- Produire une documentation exhaustive des mesures prises
- Effectuer une formation au RGPD aux entreprises

Qui est concerné par l'application du principe d'accountability ?

Il est parfois difficile d'identifier les personnes concernées par le RGPD.

Conformément à l'article 5-2 du RGPD, c'est au **responsable de traitement** qu'il appartient de mettre en œuvre le principe d'accountability. Il est en effet essentiel que ce dernier veille à la mise en place des **mesures adéquates** permettant d'assurer **la conformité** de l'entreprise ou de l'organisme public aux règles de ce texte européen.

Bon à savoir : Tous les organismes, privés ou publics amenés à traiter des données personnelles sont concernés par le RGPD. Ces derniers peuvent être établis dans l'Union européenne ou cibler des personnes y résidant.

Comment s'applique le principe d'accountability ?

L'application du principe d'accountability passe par la mise en place de **diverses mesures** essentielles. Dans le cas où ces dernières ne seraient pas respectées, elles pourront donner lieu à **des sanctions**.

Les mesures à mettre en place

Les mesures à mettre en place afin de démontrer **le respect des règles** relatives à la protection des données au sens du RGPD sont les suivantes :

- Réduire la quantité ainsi que le type de données collectées
- Faire preuve de transparence lors du traitement des données
- Traiter les données nécessaires selon les objectifs
- Sécuriser le processus de collecte du traitement
- Avoir recours à la pseudonymisation des données
- Respecter les délais de conservation
- Adopter les dispositions garantissant l'exercice des droits des utilisateurs
- Tenir des registres de traitement
- Encadrer les traitements réalisés par les sous-traitants
- Evaluer régulièrement le niveau de protection des données
- Former et sensibiliser le personnel au RGPD
- Nommer un responsable de traitement

A noter : Le RGPD impose également la pratique d'une analyse d'impact ainsi que la désignation d'un DPO dans certaines conditions.

Quelles sanctions en cas de non-respect du principe d'accountability ?

Les entreprises ou organismes ne respectant pas les règles instituées par le RGPD s'exposent à de lourdes [sanctions](#) à **l'échelle européenne** notamment.

En effet, les organismes de contrôle des pays européens ayant adopté le règlement, en cas de non-respect de ce dernier peuvent prononcer les **sanctions administratives** et **pécuniaires** suivantes :

- Le règlement d'une amende allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel pour une entreprise
- La limitation temporaire ou définitive du traitement des données par l'organisme ou l'entreprise
- Un rappel à l'ordre

- La mise en demeure de l'organisme ou l'entreprise de se mettre en conformité

A noter : Les sanctions peuvent également être rendues publiques et avoir de lourdes conséquences pour l'image de l'organisme sanctionné.

Afin d'éviter de subir ces sanctions, il est primordial pour l'entreprise de revoir régulièrement sa [politique de confidentialité](#) et de procéder à un inventaire des traitements.

FAQ

Qu'est-ce que l'accountability RGPD ?

L'accountability RGPD signifie la responsabilisation des entreprises traitant des données personnelles. En effet, celles-ci sont dans l'obligation de mettre en place des mesures pour garantir le respect des principes du RGPD. Elles doivent également être en mesure de prouver l'existence et l'application de ces mesures.

Comment mettre en place des mesures respectant l'accountability ?

Afin de mettre en place des mesures respectant l'accountability, les organismes doivent respecter les principes de privacy by design et de privacy by default. Ils doivent également mettre en place des outils permettant une documentation tels qu'un registre des activités de traitement.

Qui est responsable de la protection des données personnelles ?

Selon l'article 5 du RGPD, les responsables de traitement ont la responsabilité de respecter les conditions imposées pour respecter la protection des données personnelles. Ainsi, tout organisme, public ou privé, concerné par le traitement de données est responsable de la protection de celles-ci.